Grover's Quantum Search Algorithm for an Arbitrary Initial Amplitude Distribution

Eli Biham[1], Ofer Biham[2], David Biron[2], Markus Grassl[3] and Daniel A. Lidar[4]
[1] *Computer Science Department, Technion, Haifa 32000, Israel*
[2] *Racah Institute of Physics, The Hebrew University, Jerusalem 91904, Israel*
[3] *Institut für Algorithmen und Kognitive Systeme, Universität Karlsruhe, Am Fasanengarten 5, D–76128 Karlsruhe, Germany*
[4] *Department of Chemistry, University of California, Berkeley, CA 94720, USA*

Grover's algorithm for quantum searching is generalized to deal with arbitrary initial complex amplitude distributions. First order linear difference equations are found for the time evolution of the amplitudes of the marked and unmarked states. These equations are solved exactly. New expressions are derived for the optimal time of measurement and the maximal probability of success. They are found to depend on the averages and variances of the initial amplitude distributions of the marked and unmarked states, but not on higher moments. Our results imply that Grover's algorithm is robust against modest noise in the amplitude initialization procedure.

It is now firmly established that there exists a gap between the computational power of quantum and classical computers. A dramatic example of the speed-up offered by quantum computers is Grover's quantum search algorithm [1,2] for finding a marked element among N possible input values, in the presence of an oracle. On average a classical computer would need $N/2$ oracle-queries, whereas a quantum computer can accomplish the same task using merely $O(\sqrt{N})$ queries. The importance of Grover's result stems from the fact that it proves the enhanced power of quantum computers compared to classical ones for a whole class of oracle-based problems, for which the bound on the efficiency of classical algorithms is known.

Grover's algorithm can be represented as searching a preimage of an oracle-computable boolean function, which can only be computed forward, but whose inverse cannot be directly computed. Such a function is $F : D \rightarrow \{0, 1\}$ where D is a set of N domain values (or states) and the preimages of the value 1 are called the *marked* states. The problem is to identify one of the marked states, i.e., some $v \in D$ such that $F(v) = 1$. Problems of this type are very common. One important example, from cryptography, is searching for the key K of the Data Encryption Standard (DES) [3], given a known plaintext P and its ciphertext C, where $F = 1$ if the pair of plaintext and ciphertext match [i.e., $E_K(P) = C$ where E_K is the encryption function] and $F = 0$ otherwise. Other examples are solutions of NP and NP-complete problems, which include virtually all the difficult computing problems in practice [4].

A large number of results followed Grover's discovery. These results include a proof [5] that the algorithm is as efficient as theoretically possible [6]; a variety of applications in which the algorithm is used in the solution of other problems [7–14]; and recently, an experimental implementation using a nuclear magnetic resonance (NMR) quantum computer [15]. Several generalizations of Grover's original algorithm have been published, the first of which dealt with the case of more than one marked state [16]. The algorithm was further generalized by allowing an arbitrary (but constant) unitary transformation to take the place of the Hadamard transform in the original setting [17].

In this Rapid Communication, we generalize Grover's algorithm by allowing for an *arbitrary complex initial amplitude distribution*. We present an exact solution for the time evolution of the amplitudes under these general initial conditions. We find that the generalized search algorithm still requires $O(\sqrt{N/r})$ iterations, where r is the number of marked states, although the maximal success probability can be small for certain unfavorable initial amplitude distributions. The case of an arbitrary initial amplitude distribution is particularly relevant in the presence of unitary errors in the gates implementing the initialization step, such as over- or under-rotations. Such errors can result in a deviation from the uniform initial amplitude distribution assumed in the usual treatment of Grover's algorithm, and as detailed below, our analysis shows that the algorithm will still work in the presence of modest errors.

We will now present the modified Grover algorithm and derive difference equations for the time evolution of the amplitudes in it. We then solve these equations exactly and analyze the results. Let $k(t)$ $[l(t)]$ denote the amplitude of the marked [unmarked] states after t iterations of the algorithm. It was shown in [16] that the amplitude of the marked states increases as: $k(t) = \sin[\omega(t + 1/2)]/\sqrt{r}$, where $\omega = 2 \arcsin(\sqrt{r/N})$. At the same time the amplitude of the unmarked states decreases as: $l(t) = \cos[\omega(t + 1/2)]/\sqrt{N - r}$. For $N \gg r$ the optimal time to measure and complete the calculation is after $T = O(\sqrt{N/r})$ iterations, when $k(t)$ is maximal. In our modified algorithm we simply omit the initialization step from Grover's original algorithm. It thus consists of the following stages:

1. Use any initial distribution of marked and unmarked states, e.g., the final state of any other quantum algorithm (do *not* initialize the system to the uniform distribution).

2. Repeat the following steps T times:

   A. Rotate the marked states by a phase of π radians.

   B. Rotate all states by π radians around the average amplitude of *all* states. This is done by (i) Hadamard transforming every qubit; (ii) rotating the $|0\rangle$ state by a phase of π radians; (iii) again Hadamard transforming every qubit.

3. Measure the resulting state.

Next, we analyze the time evolution of the amplitudes in the modified algorithm with a total of N states. Let the marked amplitudes at time t be denoted by $k_i(t)$, $i = 1, \ldots, r$ and the unmarked amplitudes by $l_i(t)$, $i = r+1, \ldots, N$, where the initial distribution at $t = 0$ is arbitrary. Without loss of generality we assume that the number of marked states satisfies $1 \leq r \leq N/2$. Let the averages of the amplitudes be denoted by

$$\bar{k}(t) = \frac{1}{r} \sum_{i=1}^{r} k_i(t)$$

for the marked states, and by

$$\bar{l}(t) = \frac{1}{N-r} \sum_{i=r+1}^{N} l_i(t)$$

for the unmarked states. The key observation is that the entire dynamics dictated by Grover's algorithm can be described in full by the time-dependence of the *averages*. Let us define

$$C(t) = \frac{2}{N} \left[(N-r)\bar{l}(t) - r\bar{k}(t) \right] . \qquad (1)$$

Consider any marked state $k_i(t)$. In each step of the algorithm this state is flipped to $k'_i(t) = -k_i(t)$, so that the marked average becomes $\bar{k}'(t) = -\bar{k}(t)$. The unmarked states, on the other hand, do not flip, so that the average over *all* states after the flip is: $x(t) = \frac{1}{N}[r\,\bar{k}'(t) + (N-r)\,\bar{l}(t)] = C(t)/2$. Rotation by π radians around the average is by definition: $k'_i(t) \rightarrow 2x(t) - k'_i(t)$ and $l_i(t) \rightarrow 2x(t) - l_i(t)$. Hence, $k_i(t) \rightarrow C(t) + k_i(t)$ and $l_i(t) \rightarrow C(t) - l_i(t)$. Therefore, the time evolution of all amplitudes (of both marked and unmarked states) is independent of the state index, and satisfies:

$$k_i(t+1) = C(t) + k_i(t) \qquad i = 1, \ldots, r \qquad (2)$$

$$l_i(t+1) = C(t) - l_i(t) \qquad i = r+1, \ldots, N. \qquad (3)$$

By averaging over the states in Eqs. (2) and (3) we find that the average marked and unmarked amplitudes obey first order linear coupled difference equations:

$$\bar{k}(t+1) = C(t) + \bar{k}(t) \qquad (4)$$

$$\bar{l}(t+1) = C(t) - \bar{l}(t). \qquad (5)$$

These equations can be solved for $\bar{k}(t)$ and $\bar{l}(t)$, and along with the initial distribution this yields the exact solution for the dynamics of all amplitudes. We proceed to solve the recursion formulae for arbitrary complex initial conditions. Let:

$$f_+(t) = \bar{l}(t) + i\sqrt{\frac{r}{N-r}}\bar{k}(t)$$

$$f_-(t) = \bar{l}(t) - i\sqrt{\frac{r}{N-r}}\bar{k}(t).$$

Using the recursion formulae (4) and (5) and a few steps of algebra employing the definition of $C(t)$ given in (1), we find that $f_+(t+1) = e^{i\omega} f_+(t)$ and $f_-(t+1) = e^{-i\omega} f_-(t)$. Here ω, which is real and satisfies

$$\cos\omega = 1 - 2\frac{r}{N}, \qquad (6)$$

is identical to the frequency found by Boyer *et al.* in [16]. The time evolution can now be written as

$$f_+(t) = e^{i\omega t} f_+(0)$$
$$f_-(t) = e^{-i\omega t} f_-(0).$$

Clearly, $|f_+(t)|$ and $|f_-(t)|$ are time independent quantities. The average amplitudes are

$$\bar{k}(t) = -i\sqrt{\frac{N-r}{4r}}\left[e^{i\omega t} f_+(0) - e^{-i\omega t} f_-(0)\right] \tag{7}$$
$$\bar{l}(t) = \frac{1}{2}\left[e^{i\omega t} f_+(0) + e^{-i\omega t} f_-(0)\right]. \tag{8}$$

Together with Eqs. (1)-(3) this provides the complete exact solution to the dynamics of the amplitudes in the generalized Grover algorithm, for arbitrary initial conditions.

We turn to an analysis of several properties of the amplitudes and to a simplification of the result describing the dynamics. Let α and ϕ (real or complex) be chosen such that $\alpha = \sqrt{f_+(0)f_-(0)}$, and $e^{2i\phi} = f_+(0)/f_-(0)$. Using Eqs. (7) and (8), the average amplitudes can be expressed concisely as follows

$$\bar{k}(t) = \sqrt{\frac{N-r}{r}}\alpha \sin(\omega t + \phi) \tag{9}$$
$$\bar{l}(t) = \alpha \cos(\omega t + \phi). \tag{10}$$

This shows that there is a $\pi/2$ phase difference between the marked and unmarked amplitudes: when the average marked amplitude is maximal, the average unmarked amplitude is minimal, and *vice versa.* [Note that when the ratio $\bar{l}(0)/\bar{k}(0)$ is real, α and ϕ become real, with $\alpha^2 = |\bar{l}(0)|^2 + |\bar{k}(0)|^2 r/(N-r)$ and $\tan\phi = \sqrt{r/(N-r)}\bar{k}(0)/\bar{l}(0)$]. Subtracting Eq. (4) from Eq. (2), and Eq. (5) from Eq. (3) one finds:

$$k_i(t+1) - \bar{k}(t+1) = k_i(t) - \bar{k}(t)$$
$$l_i(t+1) - \bar{l}(t+1) = -[l_i(t) - \bar{l}(t)].$$

This means that:

$$\Delta k_i \equiv k_i(0) - \bar{k}(0) \tag{11}$$
$$\Delta l_i \equiv l_i(0) - \bar{l}(0) \tag{12}$$

are *constants of motion.* This allows us to simplify the expression for the time dependence of the amplitudes:

$$k_i(t) = \bar{k}(t) + \Delta k_i \tag{13}$$
$$l_i(t) = \bar{l}(t) + (-1)^t \Delta l_i, \tag{14}$$

where Δk_i and Δl_i are given by the initial amplitude distribution (at $t = 0$).

Eqs. (9), (10), (13) and (14) are thus an alternative, simplified form describing the dynamics of the amplitudes. In this picture all marked states evolve in unison so it is sufficient to follow the time evolution of their average. The only feature distinguishing the states from one another is their initial deviation from the average. The same holds true for the unmarked states, up to an alternation about their average.

From Eqs. (13) and (14) it follows immediately that the variances

$$\sigma_k^2(t) = \frac{1}{r}\sum_{i=1}^{r} |k_i(t) - \bar{k}(t)|^2 \tag{15}$$
$$\sigma_l^2(t) = \frac{1}{N-r}\sum_{i=r+1}^{N} |l_i(t) - \bar{l}(t)|^2 \tag{16}$$

are time-independent. Now, when a measurement is performed at time t, the probability that a marked state will be obtained is $P(t) = \sum_{i=1}^{r} |k_i(t)|^2$. Since all the operators used are unitary, the amplitudes satisfy the normalization condition:

$$\sum_{i=1}^{r} |k_i(t)|^2 + \sum_{i=r+1}^{N} |l_i(t)|^2 = 1$$

at all times. Using $\overline{(y-\bar{y})^2} = \overline{y^2} - \bar{y}^2$ (y is a random variable), we find from Eqs. (15) and (16):

$$\sum_{i=1}^{r} |k_i(t)|^2 = r\sigma_k^2 + r|\bar{k}(t)|^2$$
$$\sum_{i=r+1}^{N} |l_i(t)|^2 = (N-r)\sigma_l^2 + (N-r)|\bar{l}(t)|^2.$$

Therefore, the probability of measuring a marked state at time t is given by

$$P(t) = P_{av} - \Delta P \cos 2[\omega t + \mathrm{Re}(\phi)] \tag{17}$$

where

$$P_{av} = 1 - (N-r)\sigma_l^2 - \frac{1}{2}\left[(N-r)\left|\bar{l}(0)\right|^2 + r\left|\bar{k}(0)\right|^2\right]$$
$$\Delta P = \frac{1}{2}\left|(N-r)\bar{l}(0)^2 + r\bar{k}(0)^2\right|.$$

The maximal value that this probability can obtain during the evolution of the algorithm is

$$P_{\max} = P_{av} + \Delta P.$$

Given an arbitrary initial distributions of r marked and $N-r$ unmarked states, with known averages $\bar{k}(0)$ and $\bar{l}(0)$ respectively, the optimal measurement times are after

$$T = [(j+1/2)\pi - \mathrm{Re}(\phi)]/\omega$$

iterations, for $j = 0, 1, 2, ...$ when the probability of obtaining a marked state is $P_{\max}$. An important conclusion is that to determine the optimal measurement times, all one needs to know are the average initial amplitudes and the number of marked states. Expanding ω in the expression for T in $r/N \ll 1$ (at $j = 0$) one finds that the number of iterations before the optimal measurement probability $P_{\max}$ is obtained is $O(\sqrt{N/r})$. However, the value of $P_{\max}$ can vary significantly, depending on the statistical properties (average and variance) of the initial amplitude distribution. The expected number of repetitions of the entire algorithm until a marked state is obtained is $1/P_{\max}$.

We next consider the shapes generated in the complex plane during the time evolution of $\bar{k}(t) = \{\mathrm{Re}[\bar{k}(t)], \mathrm{Im}[\bar{k}(t)]\}$ and $\bar{l}(t) = \{\mathrm{Re}[\bar{l}(t)], \mathrm{Im}[\bar{l}(t)]\}$. Eqs. (9) and (10) turn out to be identical to the equations that describe the polarization of electromagnetic plane waves [18]. By this analogy, the contours generated by these equations are ellipses in the complex plane. The major axis of the ellipse of $\bar{l}(t)$ subtends an angle η with the real axis, where η is given by $e^{i\eta} = \alpha/|\alpha|$. The length of the major [minor] axis of the ellipse is $a = |\alpha| \cosh(\mathrm{Im}\phi)$ [$b = |\alpha| \sinh(\mathrm{Im}\phi)$]. Here α and ϕ are the parameters which appear in Eqs. (9) and (10). The ellipse of $\bar{k}(t)$ has a similar shape, but its major axis subtends an angle $\eta + \pi/2$ with the real axis and its major and minor axes are longer by a factor of $\sqrt{(N-r)/r}$.

When the ratio $\bar{l}(0)/\bar{k}(0)$ is real, one can easily show that $|f_+(0)| = |f_-(0)|$. In this case the amplitudes evolve along a straight line in the complex plane, in analogy to the case of linear polarization of light, and $P_{\max} = 1 - (N-r)\sigma_l^2$. The best case, in which $P_{\max} = 1$, is obtained for Grover's original (uniform amplitudes) initialization, where $\sigma_l^2 = 0$.

A limit in which the algorithm is totally useless is obtained when either $f_+(0) = 0$ or $f_-(0) = 0$. In this case the success probability $P(t)$ remains constant during the evolution of the algorithm. This corresponds to the case of circular polarization of light. The worst case appears when $P_{\max} = P(t) = 0$ for any t. In this case, which is obtained when $\sigma_k^2 = f_+(0) = f_-(0) = \bar{k}(0) = \bar{l}(0) = 0$ and $(N-r)\sigma_l^2 = 1$, the algorithm can never find the marked states.

Finally, consider the case where the average and variance of the initial amplitude distribution are *not* known, but different runs of the algorithm use initial amplitudes drawn from the same distribution. Naively, one could pick a random number of iterations T_r and thus find a marked state with probability $P(T_r)$. Correspondingly, the expected number of repetitions of the entire algorithm using the same T_r would be $1/P(T_r)$ until a marked state is found. However, $P(T_r)$ could be very small. A better strategy is now shown. From Eqs. (6) and (17) it follows that the period of oscillation of $P(t)$ depends only on r/N, while the details of the initial amplitude distribution are all in the phase ϕ. Consider the case where one runs the algorithm twice, taking measurements at times T_1 and T_2 respectively, where $T_2 - T_1 = \pi/(2\omega)$. From Eq. (17) it is clear that in one of the two measurements $P(T) \geq P_{av} \geq P_{max}/2$. In this case we need twice as many repetitions to obtain at least half the success probability compared to the case when the optimal measurement time is known. The slowdown is thus at most a factor of four.

In this work we generalized Grover's quantum search algorithm to apply for initial input distributions which are non-uniform. In fact, it was shown that by simply omitting the first step of Grover's original algorithm, wherein a uniform superposition is created over all elements, a more general algorithm results which applies to *arbitrary* initial distributions. To analyze the algorithm, we found that the time evolution of the amplitudes of the marked and unmarked states can be described by first-order linear difference equations with some special properties. The most important of these is that all amplitudes essentially evolve uniformly, with the dynamics being determined completely by the average amplitudes. This observation allowed us to find an exact solution for the time-evolution of the amplitudes. A significant conclusion from this solution is that generically the generalized algorithm also has an $O(\sqrt{N/r})$ running time, thus being more powerful than any classical algorithm designed to solve the same task. An important future application of these results is in the study of the robustness of Grover's algorithm against errors in the unitary operations used to implement the algorithm. Our results imply that the algorithm can tolerate a moderate amount of noise in the amplitude initialization procedure. Work extending these results to the case of errors in the inversion about average step, and in the case of an arbitrary unitary transformation, is in progress.

This work was initiated during the Elsag-Bailey – I.S.I. Foundation research meeting on quantum computation in 1997, and was completed during the ensuing meeting in 1998.

[1] L. K. Grover, *Proceedings of the Twenty-Eighth Annual Symposium on the Theory of Computing*, ACM Press (New York, 1996), p. 212.

[2] L. K. Grover, Phys. Rev. Lett. **79**, 325 (1997).

[3] D.R. Stinson, *Cryptography: Theory and Practice* (C.R.C. Press, 1995).

[4] M.R. Garey and D.S. Johnson, *Computers and Intractability: a Guide to the Theory of NP-Completeness* (W.H. Freeman, San Francisco, 1979).

[5] C. Zalka, (LANL preprint quant-ph/9711070).

[6] C.H. Bennett, E. Bernstein, G. Brassard and U. Vazirani, SIAM Journal on Computing **26**, 1510 (1997).

[7] C. Durr and P. Hoyer, (LANL preprint quant-ph/9607014).

[8] L. K. Grover, (LANL preprint quant-ph/9607024).

[9] L. K. Grover, Phys. Rev. Lett. **79**, 4709 (1997).

[10] G. Brassard, P. Hoyer and A. Tapp, (LANL preprint quant-ph/9705002).

[11] B.M. Terhal and J.A. Smolin, Phys. Rev. A **58**, 1822 (1998).

[12] G. Brassard, P. Hoyer and A. Tapp, Lecture Notes in Computer Science **1380** (Springer Verlag, 1998); (LANL preprint quant-ph/9805082).

[13] N.J. Cerf, L.K. Grover and C.P. Williams, (LANL preprint quant-ph/9806078).

[14] E. Farhi and S. Gutmann, Phys. Rev. A **57**, 2403 (1998).

[15] I.L. Chuang, N. Gershenfeld and M. Kubinec Phys. Rev. Lett. **80**, 3408 (1998).

[16] M. Boyer, G. Brassard, P. Hoyer and A. Tapp, Fortschr. Phys. **46**, 493 (1998).

[17] L. K. Grover, Phys. Rev. Lett. **80**, 4329 (1998).

[18] See e.g. M. Born and E. Wolf, *Principles of Optics* (Pergamon Press, London, 1959), p. 24.